2007

IT Sharps: Issues Relating to Securely Disposing of Hard Disks From Medical Information Systems

Craig Valli
Edith Cowan University

IT Sharps: Issues relating to securely disposing of hard disks from medical information systems

Craig Valli
School of Computer and Information Science
Edith Cowan University
Mount Lawley WA, Australia
c.valli@ecu.edu.au

Abstract -**Organizations worldwide are failing to adequately erase data from hard disks before disposing of them. Recent studies have uncovered significant and highly confidential data from computer hard disks for sale in the second hand market using minimal forensic recovery techniques. Increasingly medical businesses are being required to use IT based systems to deliver or receive services. Also medical records are becoming electronic in nature and have significant secondary storage requirements. Given the increased use of IT in medical practice this paper examines the issues uncovered in the studies into recovery of remnant data from hard disks. The paper also explores methods and options for the secure disposal of data in the modern medical environment.**

Keywords: sanitization, erasure, secondary memory, hard disks, medical

I. Introduction

All organisations and individuals that use computers will have to dispose of magnetic storage media at some stage due to obsolescence of the equipment. Many organisations or individuals will simply on sell or trade in the computer with little thought about the information that was or is still on the drive [1-10]. Recent studies [5, 6, 9, 10] have indicated significant problems with the safe and secure disposal of hard disk assets. Over 80% or more of drives examined in these studies indicate they contained information that was readily retrievable with simple forensic recovery techniques. The range and type of information uncovered in previous studies was extensive. Everything from full disclosure of personal details, corporate secrets to top secret military plans for a new destroyer has been recovered in these studies.

Increasingly medical practices are either being encouraged or forced to use information technology to make the businesses more efficient or accountable. This impetus for adoption of information technology into modern medical practices comes from several areas of influence. Governments have either mandated or provided significant financial incentive for medical practitioners to modernise their practices by installing medical information systems. As well as government forces requiring a move into information technology many of the medical supply companies in the supply chain are likewise following suit. Whether it be physical goods such as pharmaceutical or the provision of knowledge such as test results for pathology or x-ray these stakeholders are increasingly requiring delivery of goods and services via IT enabled systems. This means that a modern medical practice will have significant levels of computers and storage hardware. This hardware being used is not only for the storage and retrieval of the patient records but also financial details, business records and variety of highly confidential material.

As a result of these trends medical practices are not immune to the threat of discovery of information from remnant data on storage media. This paper will outline the problem, the threat and steps for reduction of the threat.

II. Formatted is not Erased!

One of the common problems with this is that people believe that once a hard disk has been formatted that the information has been expunged, which is not true. Older low-level formatting routines used early on in computing to format disks did erase the contents of the drive however that is no longer the case.

When a drive is formatted by a modern operating system it is done as high-level formatting. This wipes out the parts of the hard drive that contain the control structures and metadata that maps data onto the disk such as the File Allocation Table, Directory Map. The disk appears to the operating system as being erased having no data shown topically to the user. However, the data that was written to the hard disk is still actually contained on that hard disk as they are not overwritten. This then allows a person with some knowledge to recover data from the drive using an automated software tool or an expert with a forensic tool to recover completely the entire hard disk contents. The same concept of potential recovery applies across other secondary based memory storage devices such as USB memory sticks, digital media players, iPOD and flash memory cards.

What is of concern is that in the studies conducted [5, 6, 9, 10] most techniques for recovery were simple and did not require extensive forensics skills. In several cases, this was achieved by powering up the hard disk and allowing the operating systems to boot. The majority of disks in the studies had simply been formatted.

A further compounding factor is the increasing size of memory storage devices. Currently the minimum hard disk size that can be purchased as a new device is 80 GB and this drive will typically cost less than AU$80. Most modern operating systems even with productivity tools and applications installed may use less than half this hard disk capacity.

Furthermore, it is highly unlikely that a conventional user would at any stage create 40 GB of documents before the hard disk or computer was replaced. This was not the case previously where hard disks were small 2 -10 GB in size and expensive. This normally meant that a hard disk at some stage would become full overwriting already used areas of hard disk, thereby it would not contain a complete record of the computers usage. This means that most modern hard disks in corporate machines will most probably contain a complete record of the machines usage.

If we take the case of a medical practice, this now allows a potentially malicious individual to retrieve a complete medical history for an individual from a hard disk. This is possible without ever having accessed the medical record on the server or being connected to the system at the practice.

Some people would assume it would be reasonable to say that the chances of specifically targeting such a machine/hard disk are slim if not impossible. From evidence acquired by the author at two auctions attended this calendar year two batches of machines for sale were clearly marked with asset tags as coming from a medical service providers. The drives on these machines yielded confidential patient data and financial details of the customers. These breaches were of a very serious nature. In the UK a National Health Service hard disk was also uncovered in the same collaborative study this calendar year. This hard disk likewise revealed highly confidential material relating to medical and financial records. What also makes the targeting of these systems easier is that many of the advertisements for auction items themselves will list that they have come from a specific organisation such as a bank or hospital.

III. So what constitutes cleansed

One of the remedies for this problem of remnant data is the secure erasure of the hard disk device, which is normally achieved by overwriting a hard drive mechanism several times with a random data stream. One of the paragons of the secure erasure literature Gutmann [11] stated that 35 wipes or passes of a drive made it sufficiently expensive to recover data from hard disks with conventional methods or even electromagnetic microscopy.

There are few mandated standards for the erasure of digital media available publicly. The US Department of Defense (DoD) 5220.22-M is one such publicly available standard and this has become a *de-facto* minimum standard for erasure software manufacturers. The US Department of Defense (USDOD) standard *DoD 5220.22-M* is stated as "Overwrite all addressable locations with a character, its complement, then a random character and verify" p58[12]. This standard has certain levels of passes being 3, 7 and 35 respectively. It should be noted that even at the top level of 35 passes this level of erasure is recommended for all devices except those containing Top Secret classification materials which must be disposed of by disintegration into particles. Furthermore, Gutmann in 1999 wrote an epilogue to his 1996 paper stating that 35 passes was not a conclusive way of erasing the data beyond recovery. The question posed here is what level of confidentiality or surety do we need for medical records.

One of the problems associated with erasure with such extensive wipes or passes of the drive is the actual time taken to affect an erasure. In a study done undertaken by Valli and Patak [13] modern hard disk mechanisms such as 250 GB SATA drive took over 60 hours to erase using 35 passes of random data. This time is not an insignificant amount and would significantly affect a critical path for the timely rollover of an information system. If we assume that a rollover did not start until 5 p.m. on Friday the earliest that a machine could be safely removed having been erased to this level would be 5 a.m. Monday morning assuming no failure of process or validation of same.

Total erasure can be accomplished by using a degaussing unit that applies a reverse magnetising field to the hard disk or secondary storage device. Properly applied, degaussing renders any previously stored data on magnetic media unreadable but a complication is that it typically renders the hard disk or storage device unusable. This is because the other solid state and electronic components that are contained within the device also similarly destroyed by the application of a degaussing process. The other method for rendering a hard disk incapable of revealing secrets is quite simply the total physical destruction of the hard disk mechanism. This destruction can be readily achieved with a large percussive device such as a hammer and a handheld power drill.

Both degaussing and physical destruction require the actual removal of the hard drive from the computer. These methods require physical effort to be expended which would have to be factored in is the cost of disposal via these methods. Use of these methods although highly effective may actually be in breach of corporate leasing arrangements that often require the return of the complete computer. Hence, destruction of a hard drive deliberately may incur a financial penalty on top of the incurred labour costs for destroying the drive via these methods.

IV. Practical Remedies

In addition to erasure via verified software, one effective method in risk mitigation is the use of strong encryption on hard disks. Modern operating systems that have embedded encryption capabilities such as Windows XP or Macintosh [14, 15] that provide AES 128 bit encryption [16] go part way to providing a solution. These operating system embedded cryptographic countermeasures, while not providing drive wiping capabilities per se due to their strong encryption,

provide similar expense of recovery to a wipe performed by a software based erasure tool. Although not the focus of this paper it should be noted also that the use of cryptography in this manner will also increase the overall security of the medical information systems through increased confidentiality.

When using such embedded software based options, there is some ability to recover temporary files that may have been remnant in areas other than the user's directory on the hard disk. The user's directory is where most of these tools apply encryption. The other potential places of unencrypted data left behind by these encryption utilities are client or database temporary directories, web browsers directories, word processors caches or temporary file locations to name a few. If using software based cryptographic measures as a substitute for erasure or destruction then steps should be taken to ensure that these areas do not contain confidential or compromising records or fragments.

Hardware based cryptographic systems such as Silicon Data Vault [17] or the new Seagate *Momentus* hard disk that features technology called *DriveTrust* both offer complete hard disk encryption [18]. These types of technology provide complete protection from recovery of remnant data by forensic techniques. The cost of these solutions is dropping to levels where they are effective on a risk versus cost basis even for small medical practices.

Legislated requirement to cleanse is touted as a countermeasure or mitigation of risk in this area. However, in the studies into remnant data in the UK and the US where there are legislated requirements to destroy confidential data on hard disks the study uncovered disks that contained confidential information that breached these laws. In of itself the law in this regard does not provide a viable or realistic mechanism until cases are pursued and prosecuted under these laws. For example, to date in the UK the enforcement of the Data Protection Act has been criticised for being too lenient and at best credited with trying to establish a de-facto three strikes policy for offending organisations [19]. However, the US and UK are ahead of Australia where no specific law exists in this regard.

V. Conclusion

It could be reasonably argued with the highly sensitive and confidential information that a medical practitioner would hold on the computer that disposal of secondary memory by disintegration should be mandated. Failing this the use of hardware based cryptographic systems also provides strong protection against recovery of remnant data.

Software based wiping of the hard disk is effective at erasing secondary memory devices beyond a level where recovery by conventional methods is impossible or infeasible for individuals. However, as outlined previously wiping times for modern mechanisms are potentially anachronistic with modern organisations practices of IT rollout and replacement negatively impacting on rollover timelines. Legislation has largely failed due to soft enforcement regimes this needs to significantly change for it to become effective.

This issues aside though it should not be a reason for risking an enterprise or an individuals' privacy for procedural expediency. It is imperative given the increasingly substantive evidence that organizations are failing to securely disposal of secondary storage media that medical organizations adopt similarly stringent regimes of disposal for their IT sharps as they have for medical sharps Failure to adopt such measures so could have similarly catastrophic outcomes for all concerned.

VI. References

[1] Anonymous, "The Danger of Unsanitized Hard Drives," in *Info - Tech Advisor Newsletter*, 2003, pp. 1.

[2] Anonymous, "ID theft tops fraud list again," *ABA Bank Compliance*, vol. 24, pp. 5, 2003.

[3] M. de Paula, "Security: Risk Of Improper Disposal Of Computer Trash Grows ; Wamu found out the hard way that special care is necessary when discarding software and hardware," *Bank Technology News*, vol. 17, pp. 12, 2004.

[4] M. de Paula, "One Man's Trash Is... Dumpster-diving for disk drives raises eyebrows," *USBanker*, vol. 114, pp. 12, 2004.

[5] S. L. Garfinkel and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practise," *IEEE Security and Privacy*, vol. 1, 2003.

[6] A. Jones, Valli, C., Sutherland, I. and Thomas, P "The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market," *Journal of Digital Forensics, Security and Law*, vol. 1, pp. 23-36, 2006.

[7] R. Rohan, "The ghost of information past," *Black Enterprise*, vol. 33, pp. 47, 2002.

[8] T. Spring, "Hard drives exposed," in *PC World*, vol. 21, 2003, pp. 22.

[9] C. Valli, "Throwing the Enterprise out with the Hard Disk," presented at 2nd Australian Computer, Information and Network Forensics Conference, Fremantle, Western Australia, 2004.

[10] C. Valli and A. Jones, "A UK and Australian Study of Hard Disk Disposal," presented at 3rd Australian Computer, Information and Network Forensics Conference, Edith Cowan University, Perth, Western Australia, 2005.

[11] P. Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory," presented at Sixth USENIX Security Symposium, San Jose, CA, 1996.

[12] D. o. Defense, "DoD 5220.22-M: National Industrial Security Program Operating Manual," Department of Defense 1997.

[13] C. Valli and P. Patak, "An investigation into the efficiency of forensic erasure tools for hard disk mechanisms," presented at 3rd Australian Computer, Information and Network Forensics Conference, Edith Cowan University, Perth, Western Australia, 2005.

[14] www.apple.com, "Apple - Mac OS X - FileVault," 2007.

[15] www.microsoft.com, "Microsoft Windows XP - Encrypting File System overview," 2007.

[16] NIST, "FIPS-197: Advanced Encryption Standard," N. I. o. S. a. T. (NIST), Ed.: National Institute of Standards and Technology (NIST), 2001.

[17] www.securesystems.com.au, "Secure Systems - Silicon Data Vault," 2006.

[18] www.seagate.com, "Seagate Technology - Momentus® Hard Drive Family," 2007.

[19] www.theregister.co.uk, "Orange and Littlewoods breach Data Protection Act, says ICO | The Register," 2007.